(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 550 786 A1

(12) **EUROPEAN PATENT APPLICATION**
published in accordance with Art. 153(4) EPC

(43) Date of publication:
09.10.2019 Bulletin 2019/41

(21) Application number: **17886998.8**

(22) Date of filing: **11.09.2017**

(51) Int Cl.:
H04L 29/06 *(2006.01)*

(86) International application number:
PCT/CN2017/101307

(87) International publication number:
WO 2018/120913 (05.07.2018 Gazette 2018/27)

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
MA MD

(30) Priority: **28.12.2016 CN 201611238763**

(71) Applicant: **Huawei Technologies Co., Ltd.**
Longgang District
Shenzhen, Guangdong 518129 (CN)

(72) Inventors:
- **ZHANG, Dacheng**
  Shenzhen
  Guangdong 518129 (CN)
- **FU, Tianfu**
  Shenzhen
  Guangdong 518129 (CN)
- **ZHOU, Chong**
  Shenzhen
  Guangdong 518129 (CN)

(74) Representative: **Gill Jennings & Every LLP**
The Broadgate Tower
20 Primrose Street
London EC2A 2ES (GB)

(54) **CERTIFICATE ACQUISITION METHOD, AUTHENTICATION METHOD AND NETWORK DEVICE**

(57) This application provides a certificate obtaining method, an authentication method, and a network device, to improve control over operation permission of an APP on an API. According to the method, a network device sends certificate application information including an APP to a certificate generation device, and the certificate generation device generates a certificate according to the APP and sends the generated certificate to the network device. The certificate is used for permission authentication when the APP accesses an API of a controller. The certificate includes one or more of (a) to (c): (a) information about operation permission of the APP on N application programming interfaces APIs of the controller, (b) identifiers of L APIs that are of the N APIs and that the APP has permission to operate, and (c) identifiers of R APIs that are of the N APIs and that the APP has no permission to operate, where N is a natural number greater than or equal to 1, L is a natural number greater than or equal to 1, L is less than or equal to N, R is a natural number greater than or equal to 1, and R is less than or equal to N.

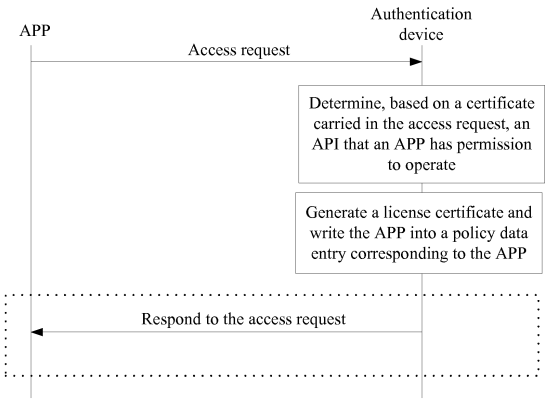

FIG. 7

EP 3 550 786 A1

Description

[0001] This application claims priority to Chinese Patent Application No. 201611238763.5, filed with the Chinese Patent Office on December 28, 2016 and entitled "CERTIFICATE OBTAINING METHOD, AUTHENTICATION METHOD, AND NETWORK DEVICE", which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] This application relates to the field of network communications technologies, and to a certificate obtaining method, an authentication method, and a network device.

BACKGROUND

[0003] Software-defined anything (English: software defined anything, SDX) is a set of all types of software-defined computing technologies. In the SDX, software plays a main role in controlling hardware. A common SDX technology includes software-defined networking (English: software-defined networking, SDN), a software-defined data center (English: software-defined data center, SDDC), software-defined storage (English: software-defined storage, SDS), and the like.

[0004] In an SDX architecture, a controller controls all hardware capabilities in a centralized manner. Moreover, the controller provides an application programming interface (English: application programming interface, API) for a user. Various applications (APP) of the user can access the API, to configure and manage a network device, a security device, a virtual machine, and the like that are controlled by the controller or to obtain network information.

[0005] However, because the APPs are from the outside of the controller, and may be developed by a third party and used by the user. It is necessary to control permissions of the APPs, so as to prevent misuse and abuse of the APIs of the controller.

SUMMARY

[0006] This application provides a certificate obtaining method, an authentication method, and a network device, to improve control over operation permission of an APP on an API.

[0007] A first aspect of this application provides a certificate obtaining method. According to the method, a network device sends certificate application information including an APP to a certificate generation device, and the certificate generation device generates a certificate according to the APP and sends the generated certificate to the network device. The certificate is used for permission authentication when the APP accesses an API of a controller. The certificate includes one or more of (a) to (c): (a) information about operation permission of the APP on N application programming interfaces APIs of the controller, (b) identifiers of L APIs that are of the N APIs and that the APP has permission to operate, and (c) identifiers of R APIs that are of the N APIs and that the APP has no permission to operate, where N is a natural number greater than or equal to 1, L is a natural number greater than or equal to 1, L is less than or equal to N, R is a natural number greater than or equal to 1, and R is less than or equal to N.

[0008] A second aspect of this application provides an authentication method. According to the method, an authentication device receives an access request message of an APP, and determines operation permission of the APP on N APIs of a controller based on information about operation permission carried in a certificate in the access request message. The certificate of the access request message includes one or more of (a) to (c).

[0009] A third aspect of this application provides a certificate generation device. The device includes a communications interface and a certificate generation module. The communications interface is configured to: receive certificate application information, and send the certificate application information to the certificate generation module, where the certificate application information includes an application APP. The certificate generation module is configured to: receive the certificate application information sent by the communications interface, and generate a certificate according to the APP in the certificate application information, where the certificate includes one or more of (a) to (c).

[0010] A fourth aspect of this application provides a network device. The network device includes a communications interface and an authentication module.

[0011] The communications interface is configured to receive an access request message of an application APP, where the access request message includes a digital certificate, and the digital certificate includes one or more of (a) to (c). The authentication module is configured to determine operation permission of the APP on the N APIs based on the information about operation permission.

[0012] According to a certificate generation method, the authentication method, and the device of this application, operation permission of an APP on an API of the controller is carried in the certificate. When accessing the API of the controller, the APP provides the certificate for the authentication device for authentication. The authentication device determines, based on the operation permission that is on the API and that is carried in the certificate, whether the APP has permission to operate the API to which the APP applies for access. This facilitates control over operation permission of the APP on the API. In addition, the method is simple, and an authentication process is simplified.

[0013] Optionally, the certificate includes (a) the information about operation permission of the APP on the N APIs of the controller, and the information about operation permission includes identifiers of the N APIs and

operation permission of the APP on each of the N APIs. In this way, the authentication device can obtain information about operation permission of the APP on all APIs, and therefore can determine whether the APP has permission to operate the API currently applied for access.

[0014] Optionally, the information about operation permission includes identifiers of M API identifier sets, an identifier of each of the M API identifier sets is used to identify operation permission on K APIs in the API identifier set, M is a natural number greater than or equal to 1, K is an integer greater than or equal to 0, and K is less than or equal to N. In this way, the authentication device can determine, based on an API identifier set carried in the certificate, APIs that the APP has permission to access or a resource that is identified by the API identifier set and that the APP has permission to access.

[0015] Optionally, the certificate includes (a) the information about operation permission of the APP on the N APIs of the controller, and the operation permission is represented by using a bitmap. In this way, occupation of a storage resource of the authentication device can be effectively reduced, and authentication efficiency can be improved.

[0016] Optionally, one or more of (a) to (c) are carried in extended information of the certificate. In this way, when authenticating the APP according to the certificate, the authentication device can determine access permission of the APP on the N APIs of the controller, so as to rapidly determine whether the APP has access permission on the API to which the APP currently applies for access.

[0017] Optionally, the network device is the controller or a part of the controller. The network device may be an authentication server.

[0018] Optionally, the network device is a software-defined networking SDN controller.

[0019] Another aspect of this application provides a network device. The network device includes a processor and a memory communicating with the processor. When running an instruction or a computer program stored in the memory, the processor may perform the foregoing certificate generation method or authentication method.

[0020] Still another aspect of this application provides a computer readable storage medium. The computer readable storage medium stores an instruction. When the instruction is run on a computer, the computer is enabled to perform the foregoing certificate generation method or authentication method.

[0021] Still another aspect of this application provides a computer program product including an instruction. When the computer program product is run on a computer, the computer is enabled to perform the foregoing certificate generation method or authentication method.

BRIEF DESCRIPTION OF DRAWINGS

[0022]

FIG. 1 is a schematic networking diagram of SDN according to an embodiment of this application;

FIG. 2 is a schematic method flowchart of a certificate obtaining method according to an embodiment of this application;

FIG. 3 is a schematic composition diagram of information that is included in a certificate and that is about operation permission of an APP on an API according to an embodiment of this application;

FIG. 4 is another schematic composition diagram of information that is included in a certificate and that is about operation permission of another APP on an API according to an embodiment of this application;

FIG. 5 is still another schematic composition diagram of information that is included in a certificate and that is about operation permission of another APP on an API according to an embodiment of this application;

FIG. 6 is a schematic composition diagram of a certificate according to an embodiment of this application;

FIG. 7 is a schematic flowchart of an authentication method according to an embodiment of this application;

FIG. 8 is a schematic composition diagram of a policy data entry according to an embodiment of this application;

FIG. 9 is a schematic composition diagram of another policy data entry according to an embodiment of this application;

FIG. 10 is a schematic composition diagram of still another policy data entry according to an embodiment of this application;

FIG. 11 is a schematic composition diagram of a certificate generation device according to an embodiment of this application; and

FIG. 12 is a schematic composition diagram of a network device according to an embodiment of this application.

DESCRIPTION OF EMBODIMENTS

[0023] The following clearly describes the technical solutions in the embodiments of the present invention with reference to the accompanying drawings in the embodiments of the present invention. Apparently, the described embodiments are merely some but not all of the embodiments of the present invention.

[0024] In this application, SDX may be SDN, an SDDC, SDS, or a software-defined infrastructure (English: software-defined infrastructure, SDI). The embodiments of this application are described below by using the SDN as an example. However, the embodiments of this application are also applicable to the SDX such as the SDDC, the SDS, or the SDI.

[0025] As shown in FIG. 1, an SDN includes a controller and X network elements controlled by the controller: a network element 1, a network element 2, ..., and a network element X. X is a natural number greater than or

equal to 1. The controller includes a data-control interface and an application-control interface. Each of the network element 1 to the network element X communicates with the controller by using the data-control interface, to receive a forwarding table sent by the controller, and forward a packet according to the forwarding table. X is a natural number greater than or equal to 1. Forwarding tables sent by the controller to different network elements may be the same or may be different. Applications, an APP 1 to an APP Z, communicate with the controller by using the application-control interface. Z is a natural number greater than or equal to 1. The controller further provides N APIs, for example, an API 1 to an API N. N is a natural number greater than or equal to 1. Each API provides one or more resources for an application to call, so that the application can control a corresponding resource by calling the API. For example, when an application APP 1 calls the API 1, the application APP 1 may forward traffic by using a bandwidth of 1 megabit per second (Mbps). Specifically, the APP 1 to the APP Z may call, by using an ACI of the controller, one or more of the API 1 to the API N that are provided by the controller, so as to operate, by using the controller, the network element 1 to a network element Y that are controlled by the controller.

[0026] Optionally, DCI is deployed with the OpenFlow (OpenFlow) Protocol. Optionally, the DCI may be further deployed with one or more of the Path Computation Element Communication Protocol (English: Path Computation Element Communication Protocol, PCEP), the Border Gateway Protocol (English: Border Gateway Protocol, BGP), the Network Configuration (NETCONF) Protocol, the Intermediate System to Intermediate System (English: Intermediate System to Intermediate System, ISIS) Protocol, and the Open Shortest Path First (Open Shortest Path First, OSPF) Protocol.

[0027] Optionally, the API may be an OpenStack (OpenStack) API, an OpenFlow API, or a Representational State Transfer (English: Representational State Transfer, RESTful) API.

[0028] In cryptology, a certificate is a public key certificate (English: public key certificate). The certificate is also referred to as a digital certificate (English: digital certificate), an identity certificate (English: identity certificate), or a security certificate. The certificate is an electronic document used to prove an identity of a public key owner. A certificate issued by a certificate issuing institution usually includes certificate validity, a public key, a subject (a certificate owner), and an algorithm used in a signature. The certificate validity represents a valid time of the certificate. The public key is a public key password used to encrypt a message. The subject (the certificate owner) is used to identify an organization using the certificate. The algorithm used in the signature is used to verify integrity of the certificate. The algorithm used in the signature may ensure that the certificate has not been tampered. A principle of the algorithm is as follows: When issuing the certificate, the certificate issuing institution calculates a hash value of the entire certificate according to a fingerprint algorithm and sends both the hash value and the certificate to a user of the certificate. When opening the certificate, the user of the certificate calculates the hash value of the certificate according to the fingerprint algorithm, and compares the calculated hash value with the hash value issued by the certificate issuing institution. If the two hash values are the same, it indicates that the certificate has not been tampered. This authentication process and standard are standardized in X.509.

[0029] As shown in FIG. 2, in a certificate obtaining method of this application, when an APP, for example, an APP 1, intends to obtain a certificate, to perform some operations by accessing one or more APIs of a controller, a network device on an owner side of the APP 1 submits the APP 1 to a certificate issuing institution. A security device of the certificate issuing institution performs security detection on the APP 1, and determines one or more of (a) to (c) based on a security detection result of the security device: (a) operation permission of the APP on each of N APIs of the controller; (b) identifiers of L APIs that are of the N APIs and that the APP has permission to operate; and (c) identifiers of R APIs that are of the N APIs and that the APP has no permission to operate. N is a natural number greater than or equal to 1. L is a natural number greater than or equal to 1, and L is less than or equal to N. R is a natural number greater than or equal to 1, and R is less than or equal to N. A certificate generation device of the certificate issuing institution generates the certificate for the APP 1. The certificate includes access permission of the APP 1 on the N APIs or a list of the L APIs that are of the N APIs and that the APP 1 has permission to operate. A certificate issuing device of the certificate issuing institution sends the certificate to the owner of the APP 1. The certificate issuing institution is an organization or a person creating a certificate. The certificate issuing institution only creates a certificate, but is not a user of the certificate.

[0030] As shown in FIG. 3, content (a) included in the certificate may include the operation permission of the APP on each of the N APIs of the controller. In FIG. 3, an APP has operation permission on an API 1 and an API 3 of the N APIs of the controller, and has no operation permission on an API 2 and an API N. Operation permission on other APIs of the N APIs is also included in the content (a).

[0031] As shown in FIG. 4, content included in the certificate is the identifiers of the L APIs that are of the N APIs and that the APP has permission to operate. In FIG. 4, assuming that an APP has operation permission only on the API 1 and the API 3 of the N APIs of the controller, and has no operation permission on other APIs of the N APIs of the controller, the certificate may include only a list of identifiers of APIs that the APP has operation permission to operate: the API 1 and the API 3.

[0032] As shown in FIG. 5, content included in the certificate is the identifiers of the R APIs that are of the N APIs and that the APP has no permission to operate. In

FIG. 5, assuming that an APP has no operation permission only on the API 1 and the API 3 of the N APIs of the controller, and has operation permission on other APIs of the N APIs of the controller, the certificate may include only a list of identifiers of APIs that the APP has no operation permission to operate: the API 1 and the API 3.

[0033] Optionally, the performing, by a security device, security detection on the APP 1 may include: performing a sandbox test on the APP 1.

[0034] Optionally, as shown in FIG. 6, the certificate may follow the X.509 standard, including:

(1) Subject (Subject): a distinguishable name of a certificate owner, where regarding a naming rule, an X.500 format is usually used;
(2) Public key information of the subject: a public key and an algorithm identifier of the subject;
(3) Certificate issuer (Issuer): including identity information and a signature of the certificate issuer;
(4) Certificate validity (Validity): valid start and ending time of the certificate;
(5) Management information: information such as a version, an encryption algorithm identifier, and a serial number of the certificate; and
(6) Extended information (Extensions) of the certificate: including a basic constraint, a related identifier, and the like.

[0035] The extended information of the certificate may include three fields: a type, defaulted or not, and a value. The type field defines a data type in an extended value field. The type may be a simple character string, value, date, or image, or a complex data type. For ease of interaction, all data types are registered with an internationally known organization. The "defaulted or not" field is a bit flag bit. When an extended identifier is "not defaulted", it indicates that a corresponding extended value is relatively important and an application cannot ignore the information. If an application using a special certificate cannot process content in this field, the application should reject the certificate. The value field includes actual data of the extended information.

[0036] One or more of (a) to (c) may be carried in the extended information of the certificate generated by the certificate generation device.

[0037] As shown in FIG. 7, when an APP, for example, an APP 1, tries to access a particular API, for example, an API 1, of a controller, an authentication device verifies whether a certificate provided by the APP 1 is valid. If the authentication device determines that the certificate provided by the APP 1 is valid, the authentication device further determines, based on (a) to (c) that are included in the certificate, API or APIs of the controller that the APP 1 has permission to access. The authentication device may be located on the controller, or may be independent of the controller, or the controller may serve as the authentication device to implement authentication of the APP.

[0038] Specifically, if the certificate includes content (a), information about operation permission of the APP on N APIs of the controller, the authentication device determines, based on the content (a), an API on which the APP has operation permission, and determines whether the API 1 is the API on which the APP has operation permission, that is, determines whether the API 1 is one of the N APIs of the controller. If the API 1 is one of the N APIs of the controller, the authentication device further determines whether permission of the APP 1 on the API 1 is "having operation permission". If the operation permission of the APP 1 on the API 1 is "having operation permission", the authentication device allows the APP 1 to operate the API 1. If the operation permission of the APP 1 on the API 1 is "having no operation permission", the authentication device does not allow the APP 1 to operate the API 1. Optionally, if the operation permission of the APP 1 on the API 1 is "having operation permission", in addition to allowing the APP 1 to operate the API 1, the authentication device may further return response information to the APP 1. The response information includes information indicating that the APP 1 has operation permission on the API 1.

[0039] Specifically, if the certificate includes content (b), identifiers of L APIs that are of the N APIs and that the APP has permission to operate, the authentication device determines, based on the content (b), whether the API that the APP tries to access is in the content (b), that is, determines whether the API 1 is in the content (b). If the API 1 is in the content (b), the authentication device determines that the APP 1 has operation permission on the API 1, and allows the APP 1 to operate the API 1. If the APP 1 is not in the content (b), the authentication device determines that the APP 1 has no operation permission on the API 1, and does not allow the APP 1 to operate the API 1. Optionally, if the APP 1 has operation permission on the API 1, in addition to allowing the APP 1 to operate the API 1, the authentication device may further return response information to the APP 1. The response information includes information indicating that the APP 1 has operation permission on the API 1.

[0040] Specifically, if the certificate includes content (c), identifiers of R APIs that are of the N APIs and that the APP has no permission to operate, the authentication device determines, based on the content (c), whether the API that the APP tries to access is in the content (c), that is, determines whether the API 1 that the APP 1 tries to access is in the content (c). If the API 1 is in the content (c), the authentication device determines that the APP 1 has no operation permission on the API 1, and does not allow the APP 1 to operate the API 1. If the APP 1 is not in the content (c), the authentication device determines that the APP 1 has operation permission on the API 1, and allows the APP 1 to operate the API 1.

[0041] According to the certificate generation method, the authentication method, and the controller of this application, operation permission of an APP on an API of the controller is carried in the certificate. When accessing

the API of the controller, the APP provides the certificate for the authentication device for authentication. The authentication device determines, based on the operation permission that is on the API and that is carried in the certificate, whether the APP has permission to operate the API to which the APP applies for access. This facilitates control over operation permission of the APP on the API. In addition, the method is simple, and an authentication process is simplified.

[0042] Optionally, if the APP 1 has operation permission on the API 1, in addition to allowing the APP 1 to operate the API 1, the authentication device may further return response information to the APP 1. The response information includes information indicating that the APP 1 has operation permission on the API 1.

[0043] Optionally, an address of the API may be a uniform resource locator (Uniform Resource Locator, URL). An API list may include one or more API identifiers. The API identifier may be a sequence number or another identifier that may be used to uniquely identify an API or a type of APIs.

[0044] Optionally, in the foregoing implementation, the "operation permission" includes "calling permission", and the "operation" includes "calling". For example, if the APP 1 has operation permission on the API 1, it indicates that the APP 1 is allowed to call the API 1; and if the APP 1 has no operation permission on the API 1, it indicates that the APP 1 is not allowed to call the API 1. Certainly, the "operation permission" may further include other possible content such as one or more of "modification permission" and "replacement permission". The "modification permission" indicates that the APP has permission to modify the API. The "replacement permission" indicates that the APP may replace the API with other content.

[0045] In an implementation, the certificate of the APP includes the content (a). The API may be a URL. To reduce the space occupied by the certificate, operation permission of the APP on each API may be represented by using a bitmap. For example, each API in an API list in the certificate of the APP is numbered by using a binary bit, and operation permission of the APP on the API corresponding to the binary bit is represented by using a value of a corresponding bit in a binary number. For example, it is assumed that the controller has four APIs, which are identified as an API 1, an API 2, an API 3, and an API 4, respectively. The API 1, the API 2, the API 3, and the API 4 may sequentially correspond to a binary bit, and a binary sequence ABCD is obtained. A corresponds to the API 1 and A is used as an identifier of the API 1. A binary value of A may represent operation permission of the APP 1 on the API 1. Cases of BCD are similar to A. Optionally, a binary bit corresponding to an API that the APP has permission to access may be set to 1, and a binary bit corresponding to an API that the APP has no permission to access is set to 0, and vice versa. For example, access permission of the APP on the API 1, the API 2, the API 3, and the API 4 corresponds to values of four binary bits, respectively. If the APP has permission to operate the API 1 and the API 2, but has no permission to operate the API 3 and the API 4, a value of operation permission of the APP on all the APIs of the controller is 1100. The certificate of the APP includes the value 1100 of the operation permission of the APP on the four APIs. When the controller determines that the value, included in the certificate provided by the APP, of the operation permission on all the APIs of the controller is 1100, the controller determines that the APP has permission to access the API 1 and the API 2 of the controller, but has no permission to access the API 3 and the API 4 of the controller.

[0046] In an implementation, if the certificate provided by the APP includes the content (b), the certificate of the APP includes one or more API identifiers. The one or more API identifiers are used to indicate that the APP has permission to operate APIs identified by the one or more API identifiers.

[0047] In an implementation, if the certificate provided by the APP includes the content (c), the certificate of the APP includes one or more API identifiers. The one or more API identifiers are used to indicate that the APP has no permission to operate APIs identified by the one or more API identifiers.

[0048] In an implementation, a plurality of APIs of the controller are divided into a plurality of API identifier sets (API Set). Each API set may include one or more API identifiers. Each API set may be used to identify a group of particular resources. In an implementation, the APP has same operation permission on APIs identified by API identifiers in the API identifier set. In another implementation, the APP may have different operation permission on the APIs identified by the API identifiers in the API identifier set. A plurality of APIs on which operation permission is different form one access permission combination. If the APP has permission to access the API identifier set, the APP has permission to operate the access permission combination. The certificate provided by the APP may include one or more API sets. For example, the controller has four APIs, and identifiers of the four APIs are API 1, API 2, API 3, and API 4, respectively. An API set 1 includes the API 1 and the API 2, an API set 2 includes the API 3, and an API set 3 includes the API 4. In an implementation, a list of API identifiers that are included in an API set is used to indicate that the APP has permission to operate APIs in the API set. In this case, if the APP 1 has permission to operate the API 1 and the API 2, but has no permission to operate the API 3 and the API 4, a certificate of the APP 1 includes only the API set 1, and does not include the API set 2 and the API set 3. In another implementation, a list of API identifiers that are included in an API set is used to indicate that the APP has no permission to operate APIs in the API set, but has permission to operate an API of the N APIs except the API set. In this case, if the APP 1 has permission to operate the API 1 and the API 2, but has no permission to operate the API 3 and the API 4, the certificate of the

APP 1 includes only the API set 2 and the API set 3, and does not include the API set 1.

[0049] In an implementation, information that is about operation permission of the APP on an API of the controller and that is obtained by the authentication device may be saved in a policy data entry manner in the authentication device, the controller, or another storage device communicating with the authentication device. A format and content of a policy data entry are shown in FIG. 8 to FIG. 10, including one or more of (a') to (c'): (a') a mapping relationship between an APP identifier and operation permission of the APP on the N APIs of the controller, (b') a mapping relationship between the APP identifier and the identifiers of the L APIs that are of the N APIs and that the APP has permission to operate, and (c') a mapping relationship between the APP identifier and the identifiers of the R APIs that are of the N APIs and that the APP has no permission to operate.

[0050] According to FIG. 8, for any APP, for example, an APP 1, a policy data entry of the APP 1 includes an APP identifier, namely, APP 1, and operation permission of the APP 1 on all APIs of the controller. Y indicates that the APP 1 has operation permission on a corresponding API, and N indicates that the APP 1 has no operation permission on the API. Certainly, the operation permission may be represented by using other symbols. For example, a number or character is used to indicate that the APP 1 has operation permission on the API, and another different number or character is used to indicate that the APP 1 has no operation permission on the API.

[0051] According to FIG. 9, for an APP, for example, an APP 1, a policy data entry of the APP 1 includes an APP identifier, namely, APP 1, and a list of identifiers of APIs that are of all APIs of the controller and on which the APP 1 has operation permission, namely, API list 1. The API list 1 includes the identifiers of the APIs on which the APP 1 has operation permission, namely, API 1, API 2, API 5, and API 7.

[0052] According to FIG. 10, for an APP, for example, an APP 1, a policy data entry of the APP 1 includes an APP identifier, namely, APP 1, and a list of identifiers of APIs that are of all APIs of the controller and on which the APP 1 has no operation permission, namely, API list 1. The API list 1 includes the identifiers of the APIs on which the APP 1 has no operation permission, namely, API 1, API 2, API 5, and API 7.

[0053] In an implementation, the authentication device may maintain only one of (a'), (b'), or (c'), or maintain only a mapping relationship between an APP and an identifier of an API set that the APP has permission to operate. The mapping relationship is relatively static, and therefore it is convenient to maintain the authentication device. Optionally, a policy data entry included in the authentication device may be aged, to decrease a size of policy data.

[0054] In an implementation, the authentication device may be an independent network device such as a server, or may be a part of the controller.

[0055] As shown in FIG. 11, the certificate generation device shown in FIG. 2 includes a communications interface 1102 and a certificate generation module 1104. The communications interface 1102 is configured to: receive certificate application information, and send the certificate application information to the certificate generation module, where the certificate application information includes an application APP. The certificate generation module 1104 is configured to: receive the certificate application information sent by the communications interface, and generate a certificate according to the APP in the certificate application information, where the certificate includes one or more of (a) to (c). The communications interface may be further configured to return the certificate including information about operation permission of the APP on an API of a controller to a network device sending the certificate application information. In addition, the certificate generation device may further include a security detection module 1106, configured to: perform security detection on the APP received by the communications interface 1102, to determine a security feature of the APP, and after determining the security feature of the APP, determine an API that is of the controller and that the APP has permission to operate. Optionally, the certificate generation device may not include the security detection module 1106. Instead, an independent security detection device is disposed outside the certificate generation device. The security detection device performs security detection on the APP received by the communications interface 1102, to determine the security feature of the APP, and after determining the security feature of the APP, determines the API that is of the controller and that the APP has permission to operate. Optionally, the certificate generation module 1104 may be implemented by using a central processing unit CPU, an application-specific integrated circuit (Application-Specific Integrated Circuit, ASIC), or a field-programmable gate array (Field-Programmable Gate Array, FPGA).

[0056] As shown in FIG. 12, the authentication device shown in FIG. 4 includes a communications interface 1202 and an authentication module 1204. The communications interface 1202 is configured to receive an access request message of an application APP, where the access request message includes a digital certificate, and the digital certificate includes one or more of (a) to (c). The authentication module 1204 is configured to determine operation permission of the APP on the N APIs based on the information about operation permission. Optionally, the authentication module 1204 may be implemented by using a CPU, an ASIC, or an FPGA. Optionally, the authentication device may be any network device that can implement the foregoing authentication method. The authentication device may be a network device independent of a controller, or may be a part of the controller. When the authentication device is a part of the controller, the authentication device may be implemented by a physical component or a software module.

[0057] Another aspect of this application provides a network device. The network device includes a processor and a memory communicating with the processor. When running an instruction or a computer program stored in the memory, the processor may perform the foregoing certificate generation method or authentication method.

[0058] Still another aspect of this application provides a computer readable storage medium. The computer readable storage medium stores an instruction. When the instruction is run on a computer, the computer is enabled to perform the foregoing certificate generation method or authentication method.

[0059] Still another aspect of this application provides a computer program product including an instruction. When the computer program product is run on a computer, the computer is enabled to perform the foregoing certificate generation method or authentication method.

[0060] All or some of the foregoing embodiments may be implemented by software, hardware, firmware, or any combination thereof. When the software is used to implement the embodiments, all or some of the embodiments may be implemented in a form of a computer program product. The computer program product includes one or more computer instructions. When the computer program instructions are loaded and executed on a computer, all or some of the procedures or functions described in the embodiments of the present invention are generated. The computer may be a general-purpose computer, a special-purpose computer, a computer network, or another programmable apparatus. The computer instructions may be stored in a computer readable storage medium, or may be transmitted by using the computer readable storage medium. The computer instructions may be transmitted from a website station, a computer, a server, or a data center to another website station, computer, server, or data center in a wired manner (for example, a coaxial cable, an optical fiber, or a digital subscriber line (DSL)) or in a wireless manner (for example, infrared, radio, or microwave). The computer readable storage medium may be any available medium that can be accessed by a computer. For example, the computer instructions may be stored or transmitted by using a magnetic medium (for example, a floppy disk, a hard disk, or a tape), an optical medium (for example, a DVD), or a semiconductor medium (for example, a solid state disk Solid State Disk (SSD)).

[0061] In the several embodiments provided in this application, it should be understood that the disclosed system, apparatus, and method may be implemented in other manners. For example, the described apparatus embodiments are merely an example. For example, the unit or module division is merely logical function division and may be other division during actual implementation. For example, a plurality of units or components may be combined or integrated into another system, or some features may be ignored or may not be performed. In addition, the displayed or discussed mutual couplings or direct couplings or communications connections may be implemented by using some interfaces. The indirect couplings or communications connections between the apparatuses or units may be implemented in electronic, mechanical, or other forms.

[0062] The units described as separate parts may or may not be physically separate, and parts displayed as units may or may not be physical units, may be located in one position, or may be distributed on a plurality of network units. Some or all of the units may be selected based on actual requirements to achieve the objectives of the solutions of the embodiments.

[0063] In addition, functional units/modules in the embodiments of the present invention may be integrated into one processing unit/module, or each of the units/modules may exist alone physically, or two or more units/modules may be integrated into one unit. The integrated unit may be implemented in a form of hardware, or may be implemented in a form of hardware in addition to a software functional unit. For example, the authentication module, the certificate generation module, and the like may all be implemented by using a CPU, an ASIC, or an FPGA.

[0064] When the foregoing integrated unit is implemented in a form of a software functional unit, the integrated unit may be stored in a computer readable storage medium. The software functional unit is stored in a storage medium and includes several instructions for instructing a computer device (which may be a personal computer, a server, a network device, or the like) to perform some of the steps of the methods described in the embodiments of the present invention. The foregoing storage medium includes various media that can store program code, such as a USB flash drive, a removable hard disk, a read-only memory (Read-Only Memory, ROM for short), a random access memory (Random Access Memory, RAM for short), a magnetic disk, or a compact disc.

[0065] The foregoing descriptions are merely example implementations of the present invention, but are not intended to limit the protection scope of the present invention. Any variation or replacement readily figured out by a person skilled in the art within the technical scope disclosed in the present invention shall fall within the protection scope of the present invention. Therefore, the protection scope of the present invention shall be subject to the protection scope of the claims.

Claims

1. A certificate obtaining method, comprising:

sending, by a network device, certificate application information to a certificate issuing device, wherein the certificate application information comprises an APP; and

receiving, by the network device, a certificate that is of the APP and that is returned by the

certificate issuing device, wherein the certificate is generated by the certificate issuing device according to the APP, and the certificate is used for permission authentication when the APP accesses an API of a controller, and
the certificate comprises one or more of (a) to (c): (a) operation permission of the APP on N application programming interfaces APIs of the controller, (b) identifiers of L APIs that are of the N APIs and that the APP has permission to operate, and (c) identifiers of R APIs that are of the N APIs and that the APP has no permission to operate, wherein N is a natural number greater than or equal to 1, L is a natural number greater than or equal to 1, L is less than or equal to N, R is a natural number greater than or equal to 1, and R is less than or equal to N.

2. The method according to claim 1, wherein the certificate comprises (a) the information about operation permission of the APP on the N application programming interfaces APIs of the controller, and the information about operation permission comprises identifiers of the N APIs and operation permission of the APP on each of the N APIs.

3. The method according to claim 1 or 2, wherein the information about operation permission comprises identifiers of M API identifier sets, an identifier of each of the M API identifier sets is used to identify operation permission on K APIs in the API identifier set, M is a natural number greater than or equal to 1, K is an integer greater than or equal to 0, and K is less than or equal to N.

4. The method according to any one of claims 1 to 3, wherein the certificate comprises (a) the operation permission of the APP on the N APIs of the controller, and the operation permission is represented by using a bitmap.

5. The method according to any one of claims 1 to 4, wherein one or more of (a) to (c) are carried in extended information of the certificate.

6. A computer readable storage medium, wherein the computer readable storage medium stores an instruction, and when the instruction is run on a computer, the computer is enabled to perform the method according to any one of claims 1 to 5.

7. A network device, comprising a processor and a memory communicating with the processor, wherein the memory stores an instruction, and when the instruction is run on a computer, the computer is enabled to perform the method according to any one of claims 1 to 5.

8. An authentication method, comprising:

receiving, by an authentication device, an access request message of an application APP, wherein the access request message comprises a digital certificate, and the digital certificate comprises one or more of (a) to (c): (a) operation permission of the APP on N application programming interfaces APIs of a controller, (b) identifiers of L APIs that are of the N APIs and that the APP has permission to operate, and (c) identifiers of R APIs that are of the N APIs and that the APP has no permission to operate, wherein N is a natural number greater than or equal to 1, L is a natural number greater than or equal to 1, L is less than or equal to N, R is a natural number greater than or equal to 1, and R is less than or equal to N; and
determining, by the authentication device, operation permission of the APP on the one or more APIs based on the information about operation permission.

9. The method according to claim 8, wherein if the digital certificate comprises (a) the information about operation permission of the APP on the N application programming interfaces APIs of the controller, the information about operation permission comprises identifiers of the N APIs and operation permission of the APP on each of the N APIs.

10. The method according to claim 8 or 9, wherein the information about operation permission comprises identifiers of M API identifier sets, an identifier of each of the M API identifier sets is used to identify operation permission on K APIs in the API identifier set, M is a natural number greater than or equal to 1, K is an integer greater than or equal to 0, and K is less than or equal to N.

11. The method according to any one of claims 8 to 10, wherein if the digital certificate comprises (a) the operation permission of the APP on the N APIs of the controller, the operation permission is represented by using a bitmap.

12. The method according to any one of claims 8 to 11, wherein one or more of (a) to (c) are carried in extended information of the certificate.

13. A computer readable storage medium, wherein the computer readable storage medium stores an instruction, and when the instruction is run on a computer, the computer is enabled to perform the method according to any one of claims 8 to 12.

14. A network device, comprising a processor and a memory communicating with the processor, wherein

the memory stores an instruction, and when the instruction is run on a computer, the computer is enabled to perform the method according to any one of claims 8 to 12.

15. A certificate generation device, comprising a communications interface and a certificate generation module, wherein
the communications interface is configured to: receive certificate application information, and send the certificate application information to the certificate generation module, and the certificate application information comprises an application APP; and
the certificate generation module is configured to: receive the certificate application information sent by the communications interface, and generate a certificate according to the APP in the certificate application information, wherein the certificate comprises one or more of (a) to (c): (a) operation permission of the APP on N application programming interfaces APIs of a controller, (b) identifiers of L APIs that are of the N APIs and that the APP has permission to operate, and (c) identifiers of R APIs that are of the N APIs and that the APP has no permission to operate, wherein N is a natural number greater than or equal to 1, L is a natural number greater than or equal to 1, L is less than or equal to N, R is a natural number greater than or equal to 1, and R is less than or equal to N.

16. The device according to claim 15, wherein if the certificate comprises (a) the information about operation permission of the APP on the N APIs of the controller, the information about operation permission comprises identifiers of the N APIs and the information about operation permission of the APP on each of the N APIs.

17. The device according to claim 15 or 16, wherein the information about operation permission comprises identifiers of M API identifier sets, an identifier of each of the M API identifier sets is used to identify operation permission on K APIs in the API identifier set, M is a natural number greater than or equal to 1, K is a natural number greater than or equal to 1, and K is less than or equal to N.

18. The device according to any one of claims 15 to 17, wherein if the certificate comprises (a) the operation permission of the APP on the N APIs of the controller, the operation permission is represented by using a bitmap.

19. The device according to any one of claims 15 to 18, wherein one or more of (a) to (c) are carried in extended information of the certificate.

20. A network device, comprising a communications interface and an authentication module, wherein
the communications interface is configured to receive an access request message of an application APP, wherein the access request message comprises a digital certificate, and the digital certificate comprises one or more of (a) to (c): (a) operation permission of the APP on N application programming interfaces APIs of a controller, (b) identifiers of L APIs that are of the N APIs and that the APP has permission to operate, and (c) identifiers of R APIs that are of the N APIs and that the APP has no permission to operate, wherein N is a natural number greater than or equal to 1, L is a natural number greater than or equal to 1, L is less than or equal to N, R is a natural number greater than or equal to 1, and R is less than or equal to N; and
the authentication module is configured to determine operation permission of the APP on the N APIs based on the information about operation permission.

21. The network device according to claim 20, wherein if the digital certificate comprises (a) the information about operation permission of the APP on the N APIs of the controller, the information about operation permission comprises identifiers of the N APIs and operation permission of the APP on each of the N APIs.

22. The network device according to claim 20 or 21, wherein the information about operation permission comprises identifiers of M API identifier sets, an identifier of each of the M API identifier sets is used to identify operation permission on K APIs in the API identifier set, M is a natural number greater than or equal to 1, K is a natural number greater than or equal to 1, and K is less than or equal to N.

23. The network device according to any one of claims 20 to 22, wherein if the digital certificate comprises (a) the operation permission of the APP on the N APIs of the controller, the operation permission is represented by using a bitmap.

24. The network device according to either of claims 22 and 23, wherein one or more of (a) to (c) are carried in extended information of the certificate.

25. The network device according to any one of claims 22 to 24, wherein the network device is the controller or a part of the controller.

26. The network device according to any one of claims 22 to 25, wherein the network device is a software-defined networking SDN controller.

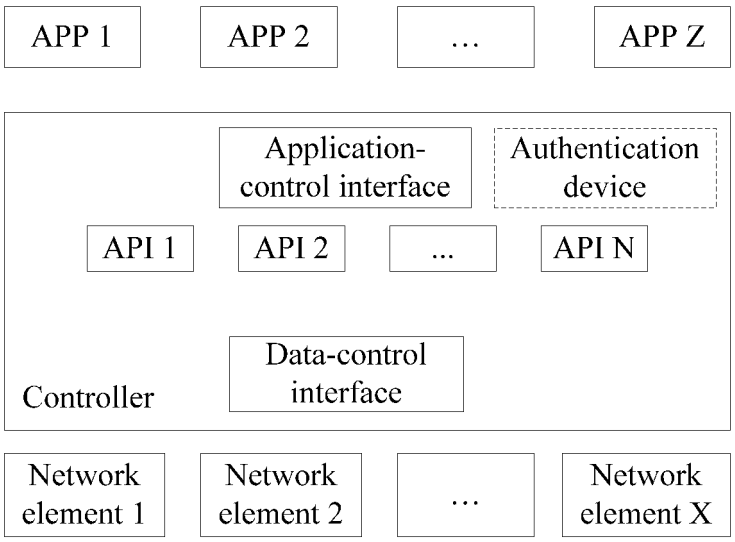
APP 1
APP 2
…
APP Z
Application-control interface
Authentication device
API 1
API 2
...
API N
Data-control interface
Controller
Network element 1
Network element 2
…
Network element X

FIG. 1

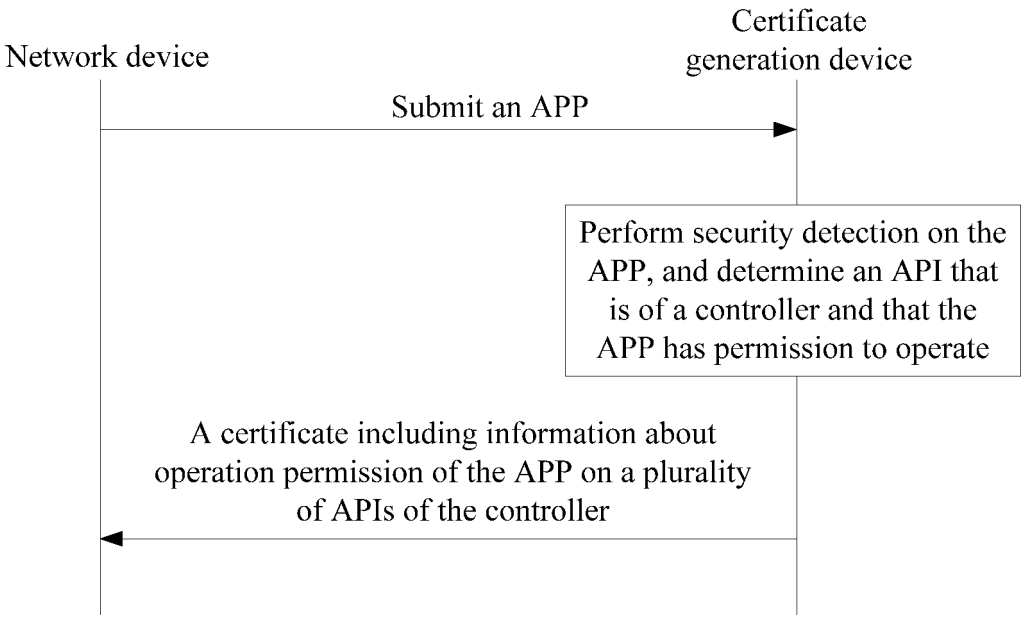
Network device
Certificate generation device
Submit an APP
Perform security detection on the APP, and determine an API that is of a controller and that the APP has permission to operate
A certificate including information about operation permission of the APP on a plurality of APIs of the controller

FIG. 2

API identifier	Operation permission
API 1	Y
API 2	N
API 3	Y
...	...
API N	N

FIG. 3

API identifier
API 1
API 3

FIG. 4

API identifier
API 1
API 3

FIG. 5

Version number
Serial number
Algorithm identifier
Identity information of an issuer
Validity
Public key of a subject
Unique identifier of an issuer
Unique identifier of a subject
Extended information
Certificate signature

FIG. 6

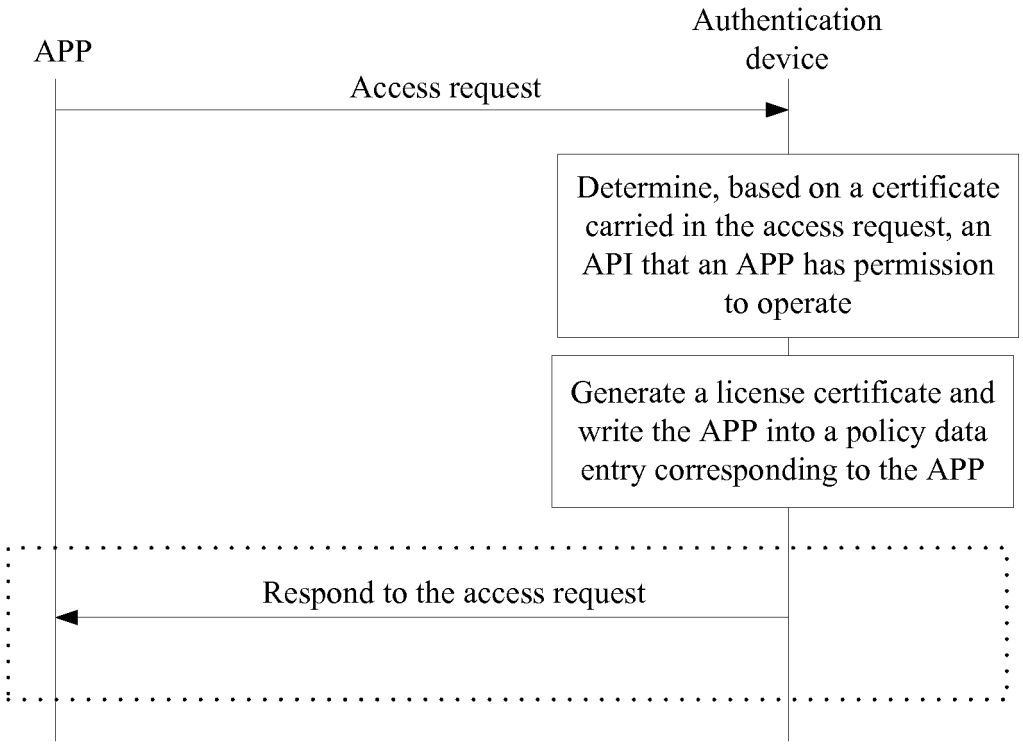
APP
Authentication device
Access request
Determine, based on a certificate carried in the access request, an API that an APP has permission to operate
Generate a license certificate and write the APP into a policy data entry corresponding to the APP
Respond to the access request

FIG. 7

APP identifier	API identifier	Operation permission
APP 1	API 1	Y
	API 2	N
	API 3	Y
	...	...
	API N	N
APP 2	API 1	N
	API 2	N
	API 3	Y
	...	...
	API N	N
APP 3	API 1	Y
	API 2	Y
	API 3	Y
	...	...
	API N	N
...	...	...
APP Z	API 1	Y
	API 2	N
	API 3	Y
	...	...
	API N	Y

FIG. 8

APP identifier	List of APIs that are allowed to be operated	
APP 1	API list 1	API 1
		API 2
		API 5
		API 7
APP 3	API list 3	API 1
		API 3
		API 4
...	...	API 2
		API 3
APP Z	API list 1	API 4
		API 6
		API 7
		...
		API 2
		API 3
		API 4
		API 6
		API 7

FIG. 9

APP identifier	List of APIs that are not allowed to be operated	
APP 1	API list 1	API 1
		API 2
		API 5
		API 7
APP 2	API list 2	API 1
		API 3
		API 4
APP 3	API list 3	API 2
		API 3
		API 4
		API 6
		API 7
...	...	...
APP Z	API list 1	API 2
		API 3
		API 4
		API 6
		API 7

FIG. 10

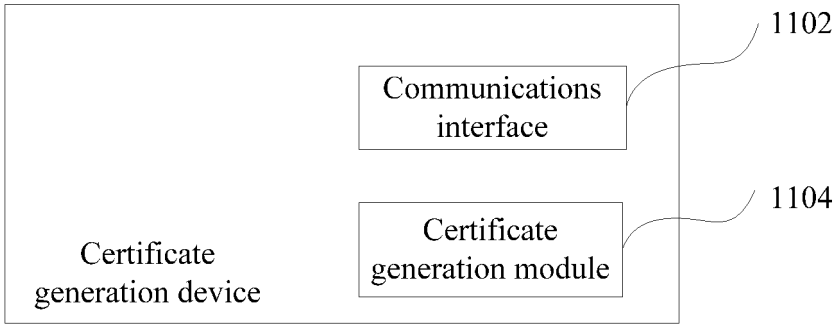
1102
Communications interface
1104
Certificate generation module
Certificate generation device

FIG. 11

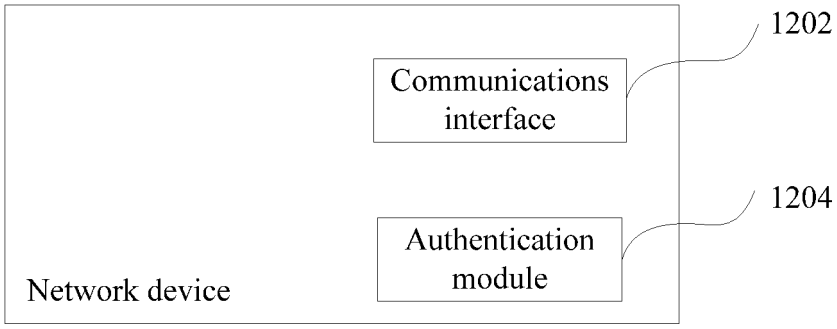
1202
Communications interface
1204
Authentication module
Network device

FIG. 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/101307

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W; H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT; WPI; EPODOC: 张大成 or 付天福 or 周冲, 鉴权 or 认证, 应用程序 or 应用编程 or APP, 应用程序接口 or 应用编程接口 or API, 权限 or 控制 or 允许 or 许可 or 证书, 软件定义一切 or SDX or 软件定义网络 or SDN or 软件定义数据中心 or SDDC or 软件定义存储 or SDS or 软件定义基础设施 or SDI, APP or program or application or software, generate or build or create or produce or product or confirm or ensure or obtain or get or got or achieve or attain or determine or decide, API or interface, control or permission or permit or allow or grant or admission or certificate or certification or license

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 102710640 A (CHINA UNITED NETWORK COMMUNICATIONS CORPORATION LIMITED), 03 October 2012 (03.10.2012), description, paragraphs [0017]-[0025] and [0042]-[0077], and figure 5	1-7, 15-19
Y	CN 102819715 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 12 December 2012 (12.12.2012), description, paragraphs [0002] and [0035]	1-7, 15-19
X	CN 105704154 A (KINGDEE SOFTWARE (CHINA) CO., LTD.), 22 June 2016 (22.06.2016), description, paragraphs [0002], [0067]-[0071] and [0096]-[0103]	8-14, 20-26
A	CN 101714201 A (RESEARCH IN MOTION LIMITED), 26 May 2010 (26.05.2010), entire document	1-26
A	EP 2787725 A1 (NIPPON HOSO KYOKAI), 08 October 2014 (08.10.2014), entire document	1-26

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 November 2017	14 December 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer NING, Bo Telephone No. (86-10) 62413288

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/101307

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102710640 A	03 October 2012	None	
CN 102819715 A	12 December 2012	WO 2014026607 A1	20 February 2014
		US 2014075574 A1	13 March 2014
CN 105704154 A	22 June 2016	None	
CN 101714201 A	26 May 2010	AU 9356301 A	02 April 2002
		AT 479931 T	15 September 2010
		ES 2545791 T3	15 September 2015
		HK 1091666 A1	14 December 2012
		HK 1091667 A1	19 November 2010
		CN 101694688 A	14 April 2010
		AT 310271 T	15 December 2005
		BR 0114066 A	10 February 2004
		HK 1055629 A1	04 May 2006
		US 2015026457 A1	22 January 2015
		EP 1626324 A2	15 February 2006
		CN 1541350 A	27 October 2004
		EP 1626325 A2	15 February 2006
		EP 1626326 A2	15 February 2006
		US 2013145150 A1	06 June 2013
		AT 553426 T	15 April 2012
		CA 2422917 A1	28 March 2002
		DE 60115072 T2	27 July 2006
		ES 2253426 T3	01 June 2006
		ES 2352556 T3	21 February 2011
		ES 2385565 T3	26 July 2012
		CN 101694687 A	14 April 2010
		HK 1153829 A1	25 July 2014
		DE 60142991 D1	14 October 2010
		ES 2465967 T3	09 June 2014
		CA 2923740 A1	28 March 2002
		WO 0225409 A2	28 March 2002
		US 2004025022 A1	05 February 2004
		EP 2306260 A2	06 April 2011
		DE 60142992 D1	14 October 2010
		HK 1154427 A1	14 November 2014
		AT 479930	15 September 2010
EP 2787725 A1	08 October 2014	US 2014344877 A1	20 November 2014
		WO 2013080632 A1	06 June 2013

Form PCT/ISA/210 (patent family annex) (July 2009)

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- CN 201611238763 **[0001]**